vertex wireless

VW210L CDMA EV-DO Rev.A Wi-Fi Router

Uživatelská příručka

2010/V1/100807



Obsah

Technické specifikace

Wi-Fi standard
IEEE 802.11g
IEEE 802.11b

Wi-Fi kanály

54Mbps	48Mbps
36Mbps	24Mbps
18Mbps	12Mbps
11Mbps	9Mbps
6Mbps	5.5Mbps
2Mbps	1Mbps

Wi-Fi zabezpečení
64/128-bit WEP
WPA-PSK
WPA-PSK2

Wi-Fi frekvence
2.4GHz to 2.483GHz

CDMA síť
VW210L
410-430MHz

Channel Bandwidth
CDMA 1.23MHz

Externí anténa
2X odnímatelné sklopné CDMA antény
Jedna Wi-Fi anténa

Indikátory led
Power – napájení
Signál

1x/EVDO	WAN
WLAN	LAN

Provozní teplota
-20 ℃ ~ +60 ℃

Skladovací teplota
-30 ℃ ~ +70 ℃

Provozní a skladovací vlhkost
5 ~ 95%

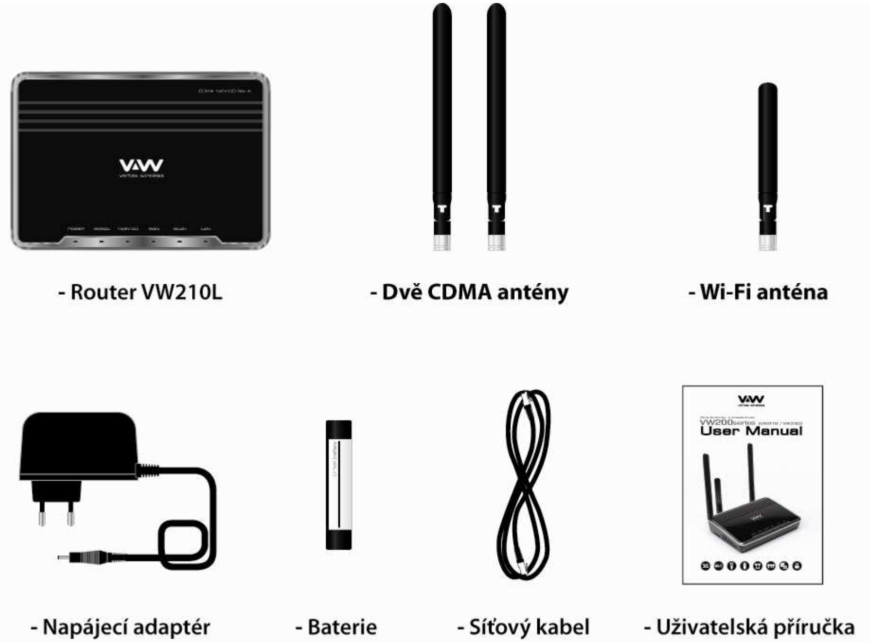
Rozměry
150(Š)x130(H)x30.5(V)mm

Provoz na baterie
Při práci: 2.5h
V klidové stavu: 3.5h

Napájecí adaptér
AC 110~240V, 50~60Hz
DC 5.0V / 2.0A

Kapitola 1. Popis produktu

Obsah balení



* pozn: baterie je umístěna v zařízení

** pozn: balení obsahuje 3 natény. 2x CDMA(velké), 1X Wi-Fi(malá)

Systémové požadavky

- PC se síťovou kartou (u) Wi-Fi nebo připojením přes konektor RJ45
- PC podporující TCP/IP protokol
- Internetový prohlížeč

Funkce

●Bezdrátová Wi-Fi síť

Router VW200 umožňuje bezdrátové připojení až 54Mbps

●Kompatibilita se zařízeními 802.11b

Router VW200 je plně kompatibilní se standardem IEEE 802.11b
a podporuje adaptéry 802.11b PCI, USB a Cardbus.

●Rozšířené funkce firewallu

Správa přístroje umožňuje nastavení řady síťových funkcí včetně:

Plánování filtrů

– Filtry mohou být nastaveny v určité dny, hodiny a minuty

Kontrola přístupu

– Kontrola obsahu pomocí MAC adresy nebo URL.

Secure Multiple/Concurrent Sessions

– RouterVW200 podporuje komunikaci přes VPN. Podpora mnohonásobných a souběžných IPSec and PPTP kanálů, vhodné pro korporátní uživatele

Popis zařízení

Přední strana routeru

Na předním panelu jsou indikátory stavu routeru



1.Power - Napájení

Stav	Popis
Nesvítí	Zařízení je vypnuto nebo není napájeno ze sítě a baterie je vybita
Svítí modře	Napájení ze sítě, baterie plně nabita
Svítí fialově	Napájení ze sítě, baterie nabita z poloviny
Svítí červeně	Napájení ze sítě, baterie vybita
Bliká modře	Nabíjení baterie
Bliká červeně	Chyba při dobíjení (například špatná baterie)

2.Signal

Stav	Popis
Nesvítí	Není signál
Svítí modře	Plný signál
Svítí fialově	Střední signál
Svítí červeně	Slabý signál

3.1x/EV-DO

Stav	Popis
Nesvítí	Připojeno k 1x
Svítí modře	Připojeno k EV-DO

4.WAN

Stav	Popis
Nesvítí	Připojeno k 1x
Svítí modře	Připojeno k EV-DO

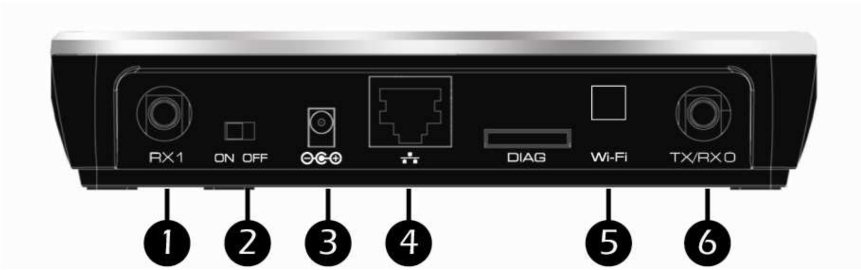
5.WLAN

Stav	Popis
Nesvítí	Wi-Fi není aktivní
Svítí modře	Wi-Fi je aktivní
Bliká modře	Wi-Fi je používáno

6.LAN

Stav	Popis
Nesvítí	PC přes kabel RJ45 není připojeno
Svítí modře	PC přes kabel RJ45 je připojeno
Bliká modře	Připojení přes LAN je používáno

Zadní strana routeru



1. Konektor pro diverzní CDMA anténu(sekundární anténa velká)
2. Tlačítko pro zapnutí
3. Konektor pro napájecí adaptér
4. Konektor RJ45 pro připojení PC
5. Konektor pro Wi-Fi anténu(malá)
6. Konektor pro CDMA anténu(hlavní velká)

** pozn: Tlačítko pro reset je umístěno na spodní straně přístroje.

Kapitola 2. Instalace

Doporučení

Router VW210L vám umožní vytvořit bezdrátovou síť a připojit se k internetu kdekoli, kde je pokrytí vašeho poskytovatele internetu. Oblast dosahu Wi-Fi bezdrátové sítě závisí na okolním prostředí(materiál zdí, budov).

1. Router by měl být umístěn v oblasti s kvalitním pokrytím CDMA.

2. Umístěte router do místa, odkud bude signál Wi-Fi překonávat co nejméně překážek(zdí).

3. Kovové materiály negativně působí na šíření Wi-Fi signálu.

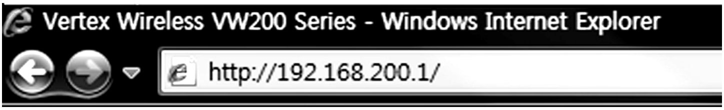
4. Umísťujte router nejméně 1-2 metry od zařízení, která vydávají elektromagnetické záření.

5. Pokud používáte bezdrátové telefony nebo zařízení na frekvenci 2.4GHz může docházet k vzájemnému rušení.

Kapitola 3. Konfigurace

Konfigurace pomocí prohlížeče

Otevřete internetový prohlížeč a zadejte adresu routeru (192.168.200.1)



Vložte přihlašovací heslo.



** Pozn: Z výroby heslo nastavené není a stačí kliknout pouze na tlačítko přihlásit

Základní nastavení

Nastavení připojení

[Nastavení internetu]

Základní nastavení: Vložte přihlašovací jméno, heslo a vytáčené číslo.
(Hodnoty jsou přednastavené operátorem)

Výběr sítě: Zvolte preferovaný mód sítě(doporučeno EVDO+1X).



Základní nastavení

[Wi-Fi nastavení]

Wi-Fi: Volba pro vypnutí nebo zapnutí Wi-Fi adaptéru zařízení.

SSID: Service Set Identifier - název vaší Wi-Fi sítě. Možno vyplnit až 32 znaků.

Zabezpečení: Volba pro vypnutí nebo zapnutí Wi-Fi zabezpečení (Z výroby je zabezpečení nastaveno WPA-PSK TKIP. Více možností jak nastavit zabezpečení naleznete v „Pokročilých nastaveních přístroje“). Po zabezpečení zapnutí se objeví pole pro zadání hesla.

Heslo: Vložte heslo pro zabezpečení WPA-PSK TKIP, pokud zabezpečení chcete používat.

[Wi-Fi nastavení]		
Wi-Fi	○ Vypnuto ⊙ Zapnuto	
SSID (název)	VW200-R06-005-009	Scan AP
Zabezpečení	○ Vypnuto ⊙ Zapnuto	Přednastavené zabezpečení WPA-PSK TKIP
Heslo	heslohesio	Musí být zadáno více než 8 znaků

Aktuální nastavení: V tomto menu najdete aktuální stav routeru.
Mód routeru, kterým je připojen k síti, přidělenou IP adresu, stav Wi-Fi sítě.

Aktuální nastavení

[Verze softwaru : 200D.CZM.005.012]

[Připojení k internetu]	
Stav připojení	1X : Idle EVDO : Connected
Kvalita signálu	2457.6 Kbps

[WAN Informace o síti]	
Dostupná sít	EVDO a 1X

[IP adresy]	
WAN IP adresa	78.136.191.110
LAN IP adresa	192.168.200.1

[Wi-Fi nastavení]	
Režim routeru	AP
Wi-Fi mód	B+G
SSID (název)	VW200-R06-005-009
Vysílání SSID	Zapnuto
Zabezpečení	WPA-PSK, TKIP

Advanced Setup

This menu provides various enhanced network function configuration and recommend to expert user. It's not necessary for all users.

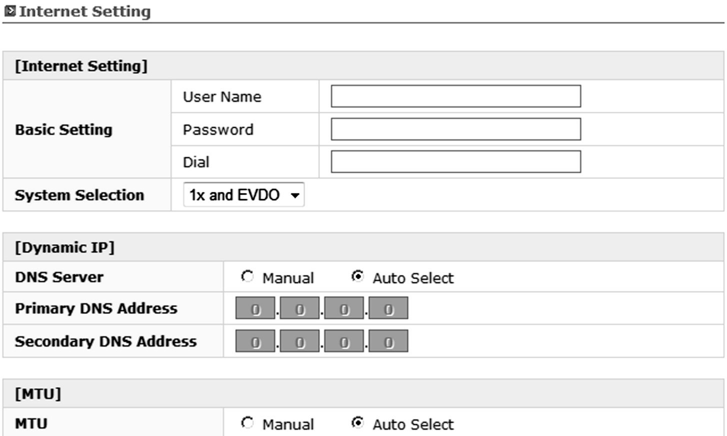
IP Setup

Internet Setting

[Internet Setting]

Basic setting: Enter your PPP user name, password and Dial (Provided by operator. Default dial: #777)

System Selection: Select a CDMA system from the drop-down menu: 1x and EVDO, 1x, and EVDO



[Dynamic IP]

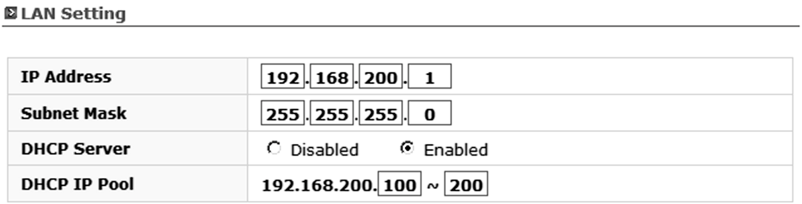
DNS Server: Select either Manual or Auto select for DNS server.

Primary DNS Address: Enter the Primary DNS server IP assigned by your ISP

Secondary DNS Address: Enter the Secondary DNS server IP assigned by your ISP (optional)

MTU: Maximum Transmission Unit – you may need to change the MTU for optimal performance with your specific ISP. Auto select is the default MTU

LAN Setting



IP Address: This is the internal IP address of the Router. The default IP address is “192.168.200.1” and it can be changed if needed.

Subnet Mask: This is a unique, advanced feature of the Router. The default is “255.255.255.0” and it can be changed if needed.

DHCP Server: The Dynamic Host Control Protocol (DHCP) server will automatically assign an IP address to the computers on the LAN/private network. Select Enabled to use DHCP server otherwise select Disabled

** Note: To use DHCP server, be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.

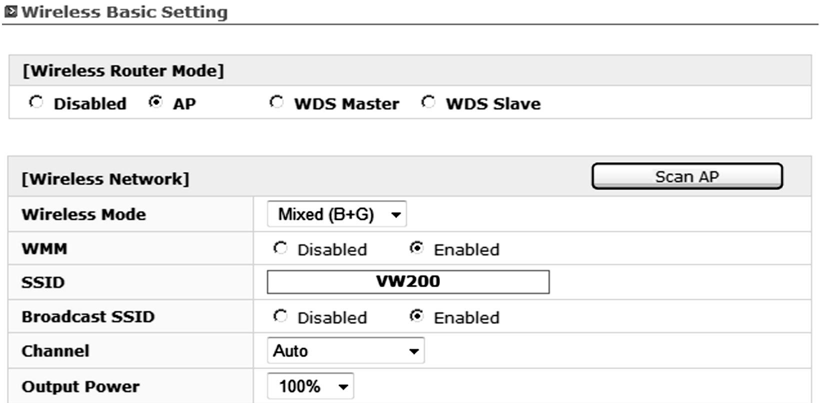
DHCP IP Pool: Enter the starting and ending IP addresses for the DHCP server’s IP assignment. The default range is 100-200.

Wireless Setup

Wireless Basic Setting

[Wireless Router Mode]

Select a Wireless Router mode from list :
Disabled / AP / WDS Master/ WDS Slave



[Wireless Network]

Wireless Mode: Select a Wireless Mode from the drop-down menu:

◎ Mixed(B+G) Mode –

Select if you are using both 802.11b and 802.11g wireless clients.

◎ G only Mode –

Select if you are using 802.11g wireless clients only.

◎ B only Mode –

Select if you are using 802.11b wireless clients only.

WMM: Wireless Multimedia Extension (WMM) mode is Power Save uses mechanisms from 802.11e and legacy 802.11 to save power (for battery powered equipment) and fine-tune power consumption. Select Enabled to use WMM otherwise select Disabled

SSID: Service Set Identifier is the name of your wireless

network. The SSID must be identical for all devices in the wireless network. Create a name using up to 32 characters. (It is case-sensitive and uses any of the characters in the keyboard)

Broadcast SSID: Select Disabled if you do not want the SSID of your wireless network to be broadcasted by the router otherwise select Enabled. If Disabled is selected, the SSID will not be detected by site survey so your wireless clients need to have the SSID manually entered to connect to the router.

Channel: A number of operating channels can be selected. If there are other wireless networks operating in your area, the channel will be set different from the channel of the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless network.

Output Power: There are a number of operating output power you can choose from. The default output power 100%. The output power can be changed if needed. For best performance, use a 100%.

ireless Distribution System(WDS) Master & Slave

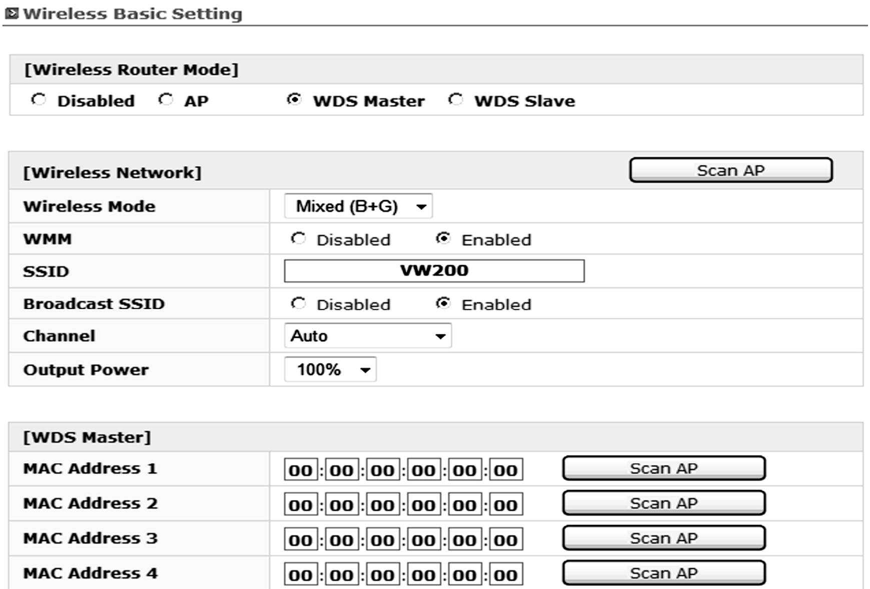
WDS is a system that enables the wireless interconnection of access points in network. It allows a wireless network to be expanded using multiple access points without need for a wired backbone to link them. It is possible to extend wireless coverage area by using more than two VW-200 (Maximum 4). WDS can be either a WDS master or remote WDS slave. WDS Master relays data between remote WDS slave, wireless clients or other relay station to either a main or other relay WDS slave. WDS Master & Slave must be configured as same SSID, Channel and security.

** Note : When you setup WDS function, please disable wireless security options of every AP's. WDS function of VW200 series is applicable with other APs which use Ralink chipset but function can be restricted for other wireless chipset.

□Setting Wi-Fi security : Disable Wi-Fi security option in each units. (You can set security option in WDS mode but recommend to set security after WDS configuration. Also you should set same security option in each Master and Slave unit.)

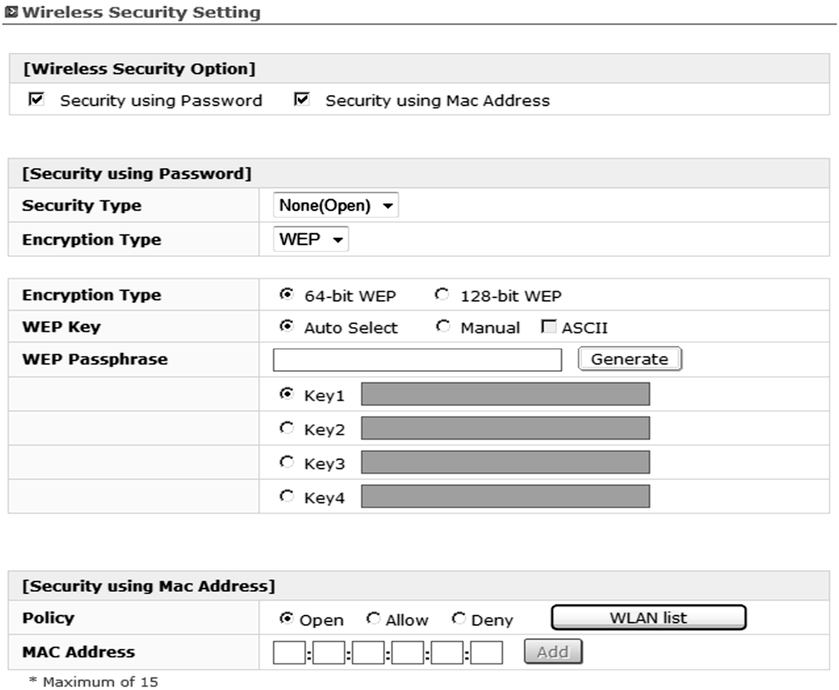
WDS Master Setting : Master mode should be set in the unit which is working with EVDO network for WAN. Connect to WEB UI using IP address, “192.168.200.1”-> Go to [Advanced Set up] -> [Wireless Set up] -> [Basic setting] -> Click [WDS Master] -> Set desired SSID and Channel. (These SSID and Channel should be same with WDS slave device.) -> Click “Scan AP” in WDS Master section -> Choose AP that you want to use as WDS Slave -> Click “Apply” to apply your configuration.

WDS Slave Setting : Connect to WEB UI using IP address, “192.168.200.1” which you want to use as WDS slave. Go to [Advanced Set up] -> [Wireless Set up] -> [Basic setting] -> Click [WDS Slave] -> Set desired SSID and Channel.(These SSID and Channel should be same with WDS Master device.) Set desired IP address of WEB UI.(Once device is operated as WDS slave, you can access WEB UI via this address.) ->Click “Scan AP” in WDS Slave section -> Choose AP that you want to use as WDS Master -> Click “Apply” to apply your configuration.



Wireless Security Setting

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home office, and small office user. At the time of this User Manual’s publication, there are two encryption methods available.



[Secu

Security Type : Select a Security Type from drop-down menu.

◎ None(open) & Shared

– In this mode, a wireless device must know the WEP key to join the network.

◎ WPA-PSK & WPA-PSK2

- In this mode, Wi-Fi protected access with Pre-Shared Key (WPA-PSK and WPA-PSK2) data encryption provides extremely strong data security, very effectively blocking eaves dropping. Uses a pass phrase or key to authenticate your wireless connection. The key is an alpha-numeric

password between 8 and 63 characters long. The password can include symbols and spaces.

Encryption Type : Select an Encryption Type from drop-down menu

◎ None(open) & Shared

◎ WEP (Wired Equivalent Privacy)

- WEP provides security by encrypting data over your wireless network so that it its protected as it is transmitted from one wireless device to another. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. In this mode, this is a common protocol that adds security to all Wi-Fi compliant wireless products. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

◎ WPA-PSK & WPA-PSK2 TKIP & AES

- Improved data encryption through the Temporal Key Integrity Protocol(TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard(AES) instead of TKIP.

[Security using Mac Address]

The MAC address security is a powerful security feature that allows you to specify which computers are allowed on the network. When you use this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each.

Policy : Select a Policy from the three different modes:

◎ Open – In this mode, there is no restriction to any device connected to the Modem whether it is through Wi-Fi or Ethernet ports.

◎ Deny – In this mode, the service table shows the client \ MAC address being blocked by the Modem.

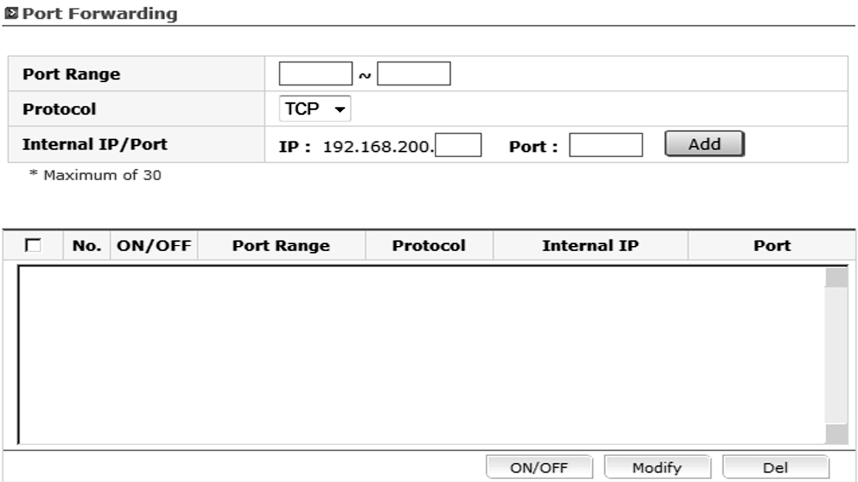
◎ Allow – In this mode, the service table shows the client MAC address allowed by the Modem.

** Note: You will not be able to delete the MAC address of the computer you are using to access the Router's administrative functions (the computer you are using now).

Traffic Control

Port Forwarding

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might make a local Web server, FTP server visible and available to the Internet. This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. You will need to contact the application vendor to find out which port settings you need. To enter settings, select the Protocol from the dropdown box, you will see a list of common applications (TCP,UCP). Select the desired applications, enter the IP address and the port number in the space provided for the internal (server) machine and click “Add” & “Apply”.



Demilitarized Zone (DMZ)

The DMZ feature is helpful when you using some on line WEB, FTP, Telnet, E-Mail conferencing application. The modem is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. Incoming traffic from the internet is usually discarded by the modem unless the traffic is a response to one of your local computers. The computer in the DMZ is NOT protected from hacker attacks.

Advanced Setup

Irregular FTP

You can use this function if you wish to connect to external irregular FTP port. You can use maximum of five irregular FTP port.

Quality of Service (QOS)

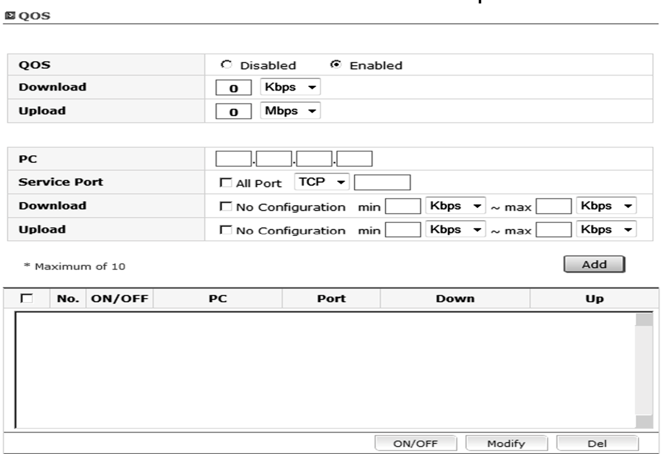
The QOS Engine option helps improve your network performance by prioritizing applications. By default the QOS Engine are disabled and application priority is not classified automatically. It guarantees the minimum speed by setting either pc or port speed and it also limits the maximum speed. It is efficient use this function when you have many users. It is only possible to manage setting for 10 pc.

Download, Upload: It is current speed of CDMA service. It is possible to manage the speed of the internet between 12Kbps and 3.1Mbps.

PC: When using a service to limit the speed of the internet connection, and you have many PCs connected to one router, then the speed of the internet slow down.

Service Port : You need to assign a unique port number to insure that you have the min speed required.

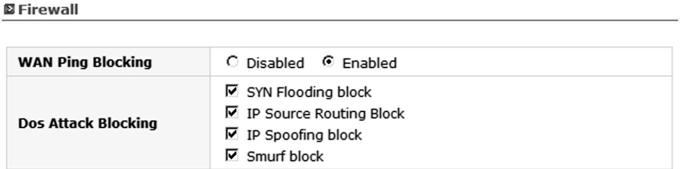
Download, Upload speed: The speed at which data can be transferred from the modem. You can limit the speed for both min & max.



Security

Firewall

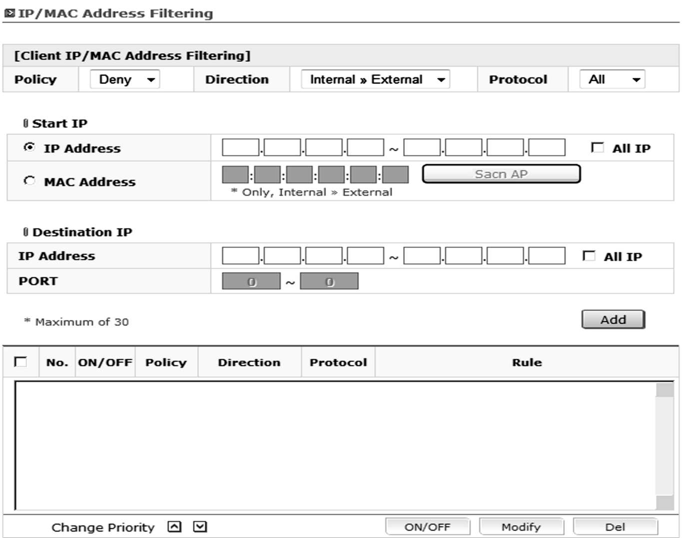
Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:
WAN Ping / SYN Flooding / IP Source Routing / IP Spoofing / Smurf Attack



You can turn the firewall functions off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

IP/MAC Address Filtering

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers by IP or MAC address specification. Available up to 30ea configuration list.



[Client IP/MAC Address Filtering]

Policy : Select filtering policy Deny or Allow

Direction

◎ Internal to External : Select if you want to apply filtering policy in the outgoing communication. (All clients are allowed in case of outgoing communication by default)

◎ External to Internal : Select if you want to apply filtering policy in the incoming communication. (All clients are restricted in case of incoming communication by default. Hence this option is valid in case of DMZ or IP Forwarding)

Protocol : Select one among of TCP / UDP / ALL. If you select ALL option, filtering policy will be applied in all protocol.

Start IP

◎ Internal to External

IP Address :	Configure internal client IP address to be restricted by filtering policy.
All IP :	Apply filtering policy in all clients.
MAC Address :	Configure internal client MAC address to be restricted by filtering policy. You can scan client MAC address using Scan AP button.

◎ External to Internal

IP Address :	Configure external IP address to be restricted by filtering policy.
All IP :	Apply filtering policy in all external IP address.
MAC Address :	Not available in this option.

Destination IP

□ Internal to External

IP Address/PORT :	Configure external IP address and Port to be restricted.
All IP :	Apply filtering in all external IP address.

□ External to Internal

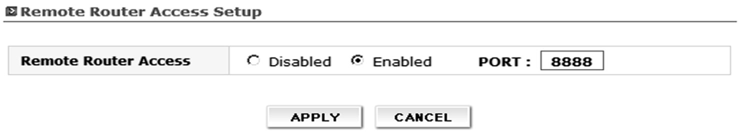
IP Address/PORT :	Configure internal client IP address and Port to be restricted.
All IP :	Apply filtering in all internal client IP address.

URL Filtering

You can block desired website URL. Once you register specified URL, clients can not access this address. Available up to 10 URL registrations.

Remote Router Access

Remote management allows you to make changes to your Router's settings from anywhere on the Internet.

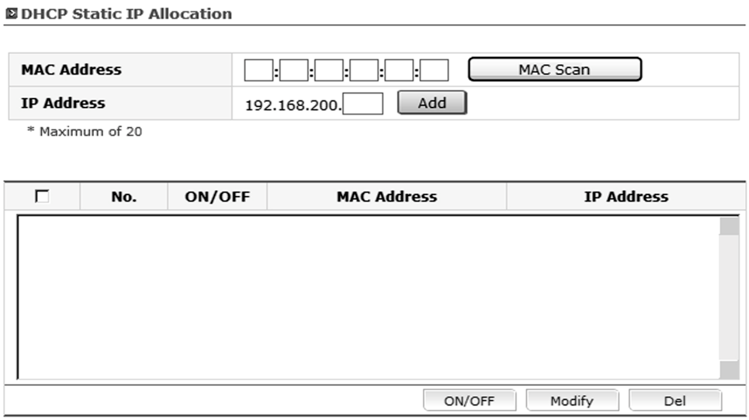


Ex) If registered DDNS Domain name is "vertexwireless.vw200.com" and you have set port number "8888" in this menu, you can access the router with this address, http://vertexwireless.vw200.com:8888.

Utility

DHCP Static IP Allocation

Use this menu if you want to assign a fixed local IP address to a MAC address.



MAC Address: Enter MAC address in the “MAC Address” field that you want to assign fixed IP address. Or you can use MAC address scan function. If you press “MAC Scan” button, router will search currently connected client’s MAC address and list up in the table.

IP Address : Select one MAC address of the list and enter the IP address you want to it to have in the “IP Address” field and press “Add” to add static IP allocation information in the table. Make sure the IP address is between the starting DHCP server’s IP address and maximum number of DHCP users range.

A list of DHCP clients and their fixed local IP address will be displayed at the bottom of the screen. If you want to remove a client from the list, click “Del”.

DDNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community. The Dynamic DNS service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you’re at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead.

To register free for your Dynamic DNS host name, please visit http://www.dyndns.org.

Setting up the Router’s Dynamic DNS update client
You must register with DynDNS.org’s free update service before using this feature. Once you have your registration, follow the directions below.



Select "Enabled" to activate DDNS service.
Press "Click" button to connect DynDNS.org's web site.
Enter the DynDNS.org domain name you set up with DynDNS.org in the "Host Name" field
Wildcards option: This setting enables or disables wildcards for your host. For example, if your DDNS address is vw200.dyndns.org and you enable wildcards, then x.vw200.dyndns.org will work as well (x is the wildcard).
To enable wildcards, select "Use Wildcards" option.
Enter your DynDNS.org user name in the "User Name" field
Enter your DynDNS.org password in the "Password" field
Press "APPLY" to update your IP address

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "APPLY" button.

UPnP

Universal Plug and Play (UPnP) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enabled" in the "UPnP" section of the "Utility" page. Click "APPLY" to save the change.

NAT-T

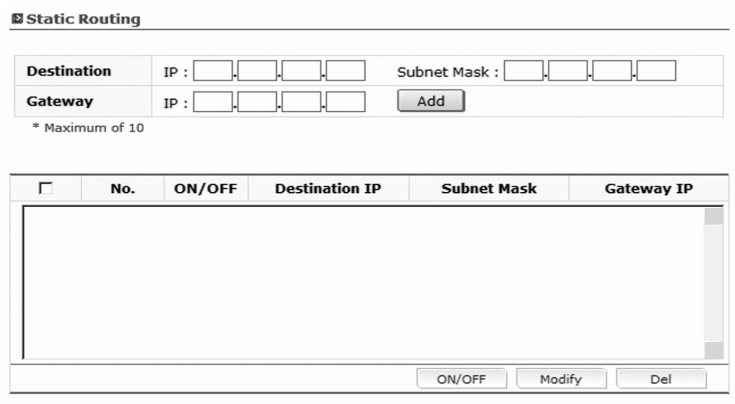
If you are using VPN, VoIP or PPTP service you can enable or disable depending on your network environment.

Wake on LAN

Wake on LAN (WOL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message. WOL must be enabled in the Power Management section of a PC motherboard's BIOS. It may also be necessary to configure the computer to reserve power for the network card when the system is shutdown. Press “MAC Scan” button to scan MAC address of currently connected client PC through RJ45 and select the scanned MAC address.
Now you connect to the router, access WEB UI and press ON button. Then the client PC will be turned on remotely using WOL. This is useful function with DDNS when you need to turn on client remotely.

Static Routing

A static IP address connection type is less common than other connection types. This is pre-determined pathway that network information must travel to reach a specific host or network.
If your ISP uses static IP addressing, you will need your IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you.



Destination : The Destination is LAN IP address of the remote network or host to which you want to assign a static route.

Subnet Mask : This determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Gateway : This is the IP address of the gateway device that allows for contact between the Router and the remote network or host. A list of Static Routing table will be displayed at the bottom of the screen. If you want to remove a client from the list, click “Del”.

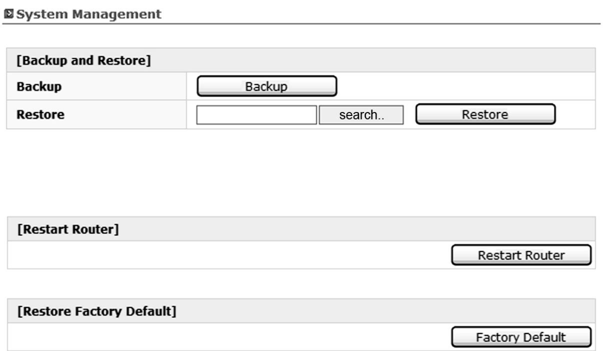
Section 4 – Administration

Administrator

Login Password

This menu is for setting up WEB UI login password.
The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into the Router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your Router.

System Management



Backup and Restore: You can save your current configuration or restore a previously saved configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

Restart Router : Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

Restore Factory Default : Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

Firmware Upgrade : From time to time, your service provider may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. When service provider releases new firmware, you can download the firmware from the service provider update website and update your Router's firmware to the latest version. In the "Firmware upgrade" page, click "Browse". A window will open that allows you to select the location of the firmware update file. A warning will be displayed while upgrading is progressed, please follow the instruction.

Section 5 – Status

Status

Status Information

You can check current gateway connection status via this menu. Detailed WAN / LAN / WLAN descriptions can be seen here.

DHCP Allocation Information

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address of the computer, the host name (if the computer has been assigned on), and the MAC address of the computer’s network interface card.

Traffic Information

A Router keeps statistics of traffic that passes through it. You are able to view the amount of packets that pass through the Ethernet and wireless portions of the network. Using Refresh button, you can reset all packet volume.

System Log

This menu displays router system log and you can save this as text file using Save button. If you want to update or reset system log, press Refresh or Delete button.

Kapitola 6 – Hlasové volání

DECT stav připojených sluchátek

Službu volání lze z přístroje VW210L využívat pomocí DECT adaptéru (není součástí standardní dodávky) a DECT telefonu(bezdrátový telefon není součástí standardní dodávky).

V menu vidíte stav přiřazených sluchátek. Tlačítkem můžete odebrat přiřazené sluchátko.

Přiřazení sluchátka

Registrace

Krok 1. Klikněte na tlačítko „Přiřadit“
Krok 2. Jakmile kliknete na tlačítko, červená kontrolka LED na DECT adaptéru začne blikat.
Krok 3. V menu bezdrátového telefonu zvolte funkci „Přihlásit“ (přihlášení k základně) a vložte správný PIN. (Přístupový kód, nastavení z výroby je "0000")
Krok 4. Po dokončení registrace, červená kontrolka LED na DECT adaptéru zhasne.

Přístupový kód

Slouží pro přiřazení sluchátka.
Zadejte nový přístupový kód (PIN), potvrďte ho a stiskněte tlačítko „Použít“

Section 7 – řešení problémů

1. Nemohu se připojit k internetovému rozhraní routeru

- Vyzkoušejte správné propojení síťovým kabelem a zda kabel není poškozen.
- Dočasně vyzkoušejte vypnutí antivirových a ostatních bezpečnostních programů.
- Zkontrolujte doporučené internetové prohlížeče
  Internet Explorer 6.0 nebo vyšší
  Firefox 1.5 nebo vyšší
  Netscape 8 nebo vyšší
  Mozilla 1.7.12 (5.0) nebo vyšší
  Opera 8.5 nebo vyšší
  Safari 1.2 nebo vyšší (s Java 1.3.1 nebo vyšší)

2. Zapomněl jsem heslo

Je nutné resetovat router. Tento proces vymaže všechna změněná uživatelská nastavení a nastaví hodnoty z výroby. Pro reset zmáčkněte tlačítko na spodní straně přístroje na 10 sekund. Po resetu nastane restartování routeru, které trvá asi 30 sekund. Původní adresa pro připojení k routeru je obnovena (192.168.200.1)

3. Proč je na modemu prostor pro SIM kartu a proč tam žadná SIM karta není?

Síť U:fon u svých fixních služeb, kam patří i Unifon, SIM karty zatím nevyužívá. Tento prostor (slot) je na modemu z důvodu snižení nákladů na výrobu modemu. (Není třeba vyrábět samostatné modely modemu pro operátory využívajicí SIM karty).

4. Kvalita signálu.

V položce základní nastavení naleznete informace o kvalitě signálu. Čím vyšší hodnota bude zobrazena, tím rychleji mohou probíhat datové přenosy.

Prohlášení o shodě

Společnost MobilKom, a.s. tímto prohlašuje, že se výrobek VW210L shoduje se základními požadavky a dalšími důležitými ustanoveními Směrnice 1999/5/EC. Prohlášení nalezneze na stránkách www.mobilkom.cz

Bezpečnostní informace

Před uvedením modemu do provozu si prostudujte tyto bezpečnostní instrukce.
Porušování těchto pravidel a instrukcí může být nebezpečné a protizákonné.

Bezpečnost letecké dopravy
Před nástupem do letadla vypněte zařízení. Používání zařízení v letadle může způsobit rušení rádiové komunikace nebo navigačního zařízení letadla.

Bezpečnost ve zdravotnických zařízeních
Před vstupem do nemocnic či jiných zdravotnických zařízení a v blízkosti lékařských přístrojů vypněte zařízení. Provoz zařízení vysílajících rádiový signál, včetně digitálních bezdrátových zařízení, může rušit lékařské přístroje citlivé na kmitočty rádiových signálů. Během pobytu v nemocnicích či jiných zdravotnických zařízeních dodržujte místní předpisy týkající se provozu zařízení.

Bezpečnost v místech odstřelu a doplňování paliva
Nepoužívejte zařízení v blízkosti míst, kde se provádí odstřel. Vypínejte zařízení v místech, kde se může vyskytovat výbušná atmosféra. Rádiové vysílání by mohlo v takových místech vyvolat výbuch či požár a způsobit tak zranění osob nebo dokonce jejich smrt. Dodržujte místní pravidla a předpisy týkající se provozu bezdrátových zařízení.

Servis
Servis Vašeho zařízení může provádět pouze kvalifikovaný servisní personál.

Při používání zařízení se řiďte následujícími pokyny
• Chraňte zařízení před nečistotou, prachem a kapalinami.
• Uchovávejte zařízení v suchu – vlhkost a kapaliny mohou vyvolat selhání zařízení a způsobují korozi jeho vnitřních obvodů.
• Chraňte zařízení před přílišným přehřátím. Zkrátit životnost elektronických součástek a způsobit deformaci nebo roztavení některých plastů.
• Nepokoušejte se zařízení otevřít pro přístup k jeho vnitřním součástkám.
Pokud zařízení nefunguje správně, zaneste jej do nejbližšího odborného servisu.

• Dbejte na to, aby zařízení neupadlo či nebylo vystaveno otřesům a vyvarujte se nešetrného zacházení se zařízením – mohlo by dojít k poškození jeho vnitřních součástek.

Pokyny pro čištění

• Vždy zařízení vypněte před jeho čištěním.

• Na čištění zařízení nepoužívejte agresivní chemikálie, silné čistící prostředky, ani rozpouštědla na bázi ropných produktů.

• Neaplikujte čistící prostředky přímo na zařízení.

UPOZORNĚNÍ

Dovozce odmítá jakoukoli odpovědnost za škody způsobené nesprávným používáním tohoto výrobku, nedodržováním pokynů v tomto návodu nebo opravou či úpravami tohoto výrobku kýmkoli jiným než technikem autorizovaný dovozcem. Dovozce neponese odpovědnost za škody způsobené na tomto výrobku používáním jakýchkoli jiných přídavných zařízení či spotřebních materiálů než těch, které jsou s ním dodávány nebo které jsou uvedeny ve specifikaci dovozce. Dovozce neponese odpovědnost za ztráty nebo ušlý zisk způsobené ztrátou dat v důsledku selhání či odstraňování selhání tohoto výrobku.

Router Vertex VW210L určený pro síť CDMA 1x/EVDO rev.A(L band).
Toto rádiové zařízení lze provozovat v rámci všeobecného oprávnění
č. VO-R20/08.2005-32.
Dovozce do České republiky: Mobilkom, a.s.

POZNÁMKY

vertex wireless

www.vwireless.co.kr